Version Date: Aug 2nd 2025

1. Purpose

The purpose of this Information Security Policy ("Policy") is to protect the confidentiality, integrity, and availability of HR2000's platform and customer data. This policy defines the controls and practices used to safeguard digital assets from threats, vulnerabilities, and breaches.

2. Scope

This policy applies to:

- All components of the platform (application, infrastructure, APIs, databases)
- All employees, contractors, vendors, and third parties accessing the system
- All devices, networks, and web services used to deliver the system

3. Information Security Objectives

- Protect customer and company data from unauthorized access or disclosure
- Maintain system uptime and data integrity
- Ensure compliance with legal, regulatory, and contractual obligations
- Establish a culture of security awareness and accountability

4. Security Principles

- Least Privilege: Access is limited to only what is necessary
- Zero Trust: Never trust, always verify all access and transactions
- Secure by Design: Security is embedded into the development lifecycle
- Continuous Monitoring: Regular assessments and improvements to security posture

5. Security Controls

5.1 Access Control

- Unique user IDs and strong passwords are required
- Apply login security with RDP port change, NLA and SSL for all remote access
- Role-based access control (RBAC) is enforced
- Inactive accounts are disabled or removed regularly

5.2 Data Protection

- Encrypted Customer Data in AES-256 for Data In Motion and Data In Use. Encrypted Data at Rest on employee distributed documents
- Data backups are performed regularly and stored securely
- Data retention policies are implemented in line with privacy and legal requirements

5.3 Application Security

- Secure coding practices are enforced (e.g., input validation, output encoding)
- Static and dynamic application security testing (SAST/DAST) is conducted

5.4 Network and Infrastructure Security

- Firewalls, intrusion detection/prevention systems (IDS/IPS), and anti-malware are used
- Server infrastructure is configured using least privilege and hardened settings
- Regular patching of systems and software

5.5 Incident Management

- All employees must report security incidents immediately
- Incident response procedures are documented and tested
- Root cause analysis is performed post-incident

5.6 Vendor and Third-Party Security

- All third-party vendors are subject to security due diligence and agreements
- Data sharing with third parties is limited and monitored

5.7 Security Awareness and Training

- Employees undergo mandatory security awareness training annually

6. Compliance

HR2000 complies with relevant laws and standards including:

- PDPA or other applicable privacy regulations
- Industry best practices for web security

7. Roles and Responsibilities

Role	Responsibilities
CISO / IT Manager	Implement and maintain security controls and awareness
Developers / Engineers	Follow secure development practices and report vulnerabilities
All Employees	Comply with security policies and report suspicious activity
Vendors / Partners	Maintain security controls as per contract and agreements

8. Policy Violations

Any violation of this policy may result in disciplinary action, including termination of employment or legal consequences. All users must read and acknowledge this policy annually.

9. Review and Update

This policy shall be reviewed annually or in response to significant changes in technology, business operations, or the threat landscape.

HR 2000 SDN BHD (475163-M)